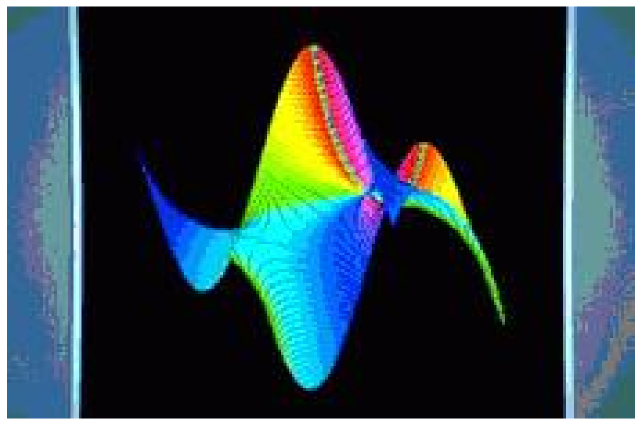
Calcul formel pour la combinatoire

Alin Bostan, Bruno Salvy

Computer algebra for Combinatorics

Alin Bostan & Bruno Salvy



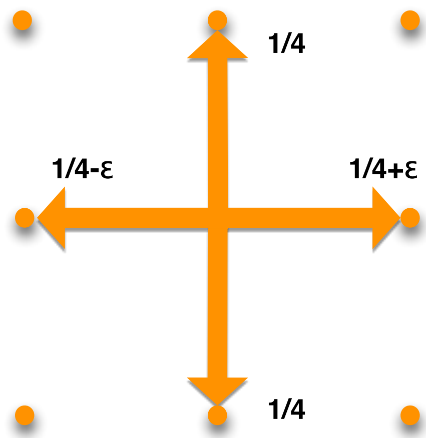
Algorithms Project, INRIA

ALEA 2012

INTRODUCTION

1. Examples

From the SIAM 100-Digit Challenge



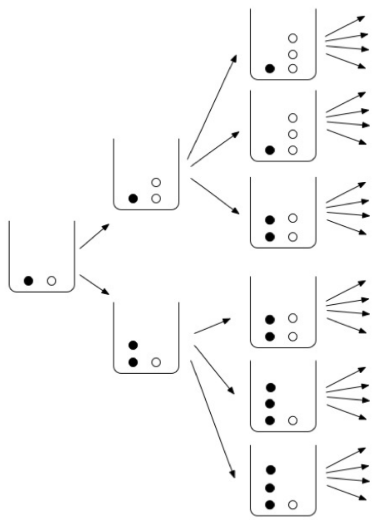
Problem 6

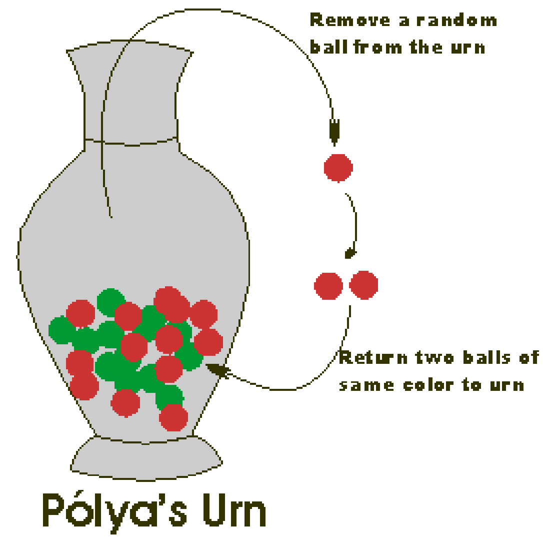
A flea starts at $(0,0)$ on the infinite two-dimensional integer lattice and executes a biased random walk: At each step it hops north or south with probability $1/4$, east with probability $1/4+\epsilon$, and west with probability $1/4-\epsilon$. The probability that the flea returns to $(0,0)$ sometime during its wanderings is $1/2$. What is ϵ?

- Computer algebra conjectures and proves

$$p(\epsilon) = 1 - \sqrt{\frac{A}{2}} \cdot {}_2F_1\left(\begin{array}{c} \frac{1}{2}, \frac{1}{2} \\ 1 \end{array} \middle| \frac{2\sqrt{1-16\epsilon^2}}{A} \right)^{-1}, \quad \text{with } A = 1 + 8\epsilon^2 + \sqrt{1-16\epsilon^2}.$$

Algebraic balanced urns





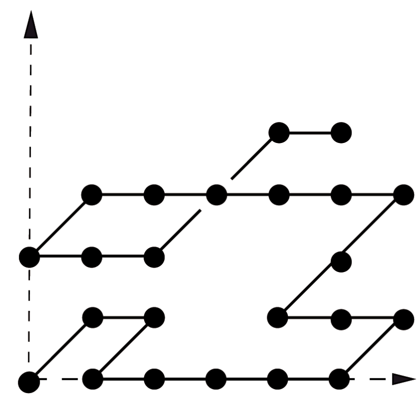
Theorem [M.Fl11]

The balanced urns class $\begin{pmatrix} 2\alpha & \beta \\ \alpha & \alpha+\beta \end{pmatrix}$, with $\alpha > 0, \beta \geqslant 0$, has an algebraic bivariate generating function.

- Computer algebra conjectures and proves larger classes of algebraic balanced urns.
- More in Basile Morcrette's talk!

Gessel's conjecture

- Gessel walks: walks in $\mathbb{N}^2$ using only steps in $\mathcal{S} = \{\nearrow, \swarrow, \leftarrow, \rightarrow\}$
- $g(i,j,n)$ = number of walks from $(0,0)$ to (i,j) with n steps in $\mathcal{S}$



Question: Nature of the generating function

$$G(x,y,t) = \sum_{i,j,n=0}^{\infty} g(i,j,n)\, x^i y^j t^n \ \in \mathbb{Q}[[x,y,t]]$$

▶ Computer algebra conjectures and proves:

Theorem [B. & Kauers 2010] $G(x,y,t)$ is an algebraic function† and

$$G(1,1,t) = \frac{1}{2t} \cdot {}_2F_1\left(\begin{matrix} -1/12 & 1/4 \\ & 2/3 \end{matrix} \,\middle|\, -\frac{64t(4t+1)^2}{(4t-1)^4}\right) - \frac{1}{2t}.$$

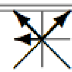
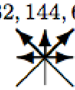
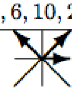
▶ A simpler variant as an exercise tomorrow.

---

†Minimal polynomial $P(x,y,t,G(x,y,t)) = 0$ has $> 10^{11}$ monomials; $\approx$30Gb (!)

Inverse moment problem for walk sequences [B., Flajolet & Penson 2011]

Question: Given (f_n), find $I \subseteq \mathbb{R}$ and $w : I \to \mathbb{R}$ s.t. $f_n = \int_I w(t)\, t^n\, dt \quad (n \geq 0)$.

Step set and walks sequence	*GF*	*Measure* $(w(t))$;	t :
A126087  $(1,1,3,5,15,29,87)$	$\frac{2z-1+\sqrt{1-8z^2}}{2z(1-3z)}$	$\frac{1}{2\pi}\frac{\sqrt{8-t^2}}{3-t}$	$[-2\sqrt{2}, 2\sqrt{2}]$
A128386  $(1,1,4,7,28,58,232,523,2092)$	$\frac{2z-1+\sqrt{1-12z^2}}{2z(1-4z)}$	$\frac{1}{2\pi}\frac{\sqrt{12-t^2}}{4-t}$	$[-2\sqrt{3}, 2\sqrt{3}]$
A151282  $(1,2,6,18,58,190,638)$	$\frac{3z-1+\sqrt{1-2z-7z^2}}{2z(1-4z)}$	$\frac{1}{2\pi}\frac{\sqrt{7+2t-t^2}}{4-t}$	$[1-2\sqrt{2}, 1+2\sqrt{2}]$
A151292  $(1,2,7,23,85,314,1207,4682)$	$\frac{3z-1+\sqrt{1-2z-11z^2}}{2z(1-5z)}$	$\frac{1}{2\pi}\frac{\sqrt{11+2t-t^2}}{5-t}$	$[1-2\sqrt{3}, 1+2\sqrt{3}]$
A129400  $(1,2,8,32,144,672,3264)$	$\frac{1-2z-\sqrt{1-4z-12z^2}}{8z^2}$	$\frac{1}{8\pi}\sqrt{(t+2)(6-t)}$	$[-2, 6]$
A151318  $(1,3,13,55,249,1131,5253)$	$\frac{5z-1+\sqrt{1-2z-15z^2}}{4z(1-5z)}$	$\frac{1}{4\pi}\sqrt{\frac{3+t}{5-t}}$	$[-3, 5]$
A060899  $(1,2,8,24,96,320,1280,4480)$	$\frac{4z-1+\sqrt{1-16z^2}}{4z(1-4z)}$	$\frac{1}{4\pi}\sqrt{\frac{4+t}{4-t}}$	$[-4, 4]$
A005773  $(1,2,5,13,35,96,267,750,2123)$	$\frac{3z-1+\sqrt{1-2z-3z^2}}{2z(1-3z)}$	$\frac{1}{2\pi}\sqrt{\frac{1+t}{3-t}}$	$[-1, 3]$
A001405  $(1,1,2,3,6,10,20,35,70,126)$	$\frac{2z-1+\sqrt{1-4z^2}}{2z(1-2z)}$	$\frac{1}{2\pi}\sqrt{\frac{2+t}{2-t}}$	$[-2, 2]$
A151281  $(1,2,6,16,48,136,408,1184)$	$\frac{4z-1+\sqrt{1-8z^2}}{4z(1-3z)}$	$\frac{1}{4\pi}\frac{\sqrt{8-t^2}}{3-t}$	$[-2\sqrt{2}, 2\sqrt{2}]$
A129637  $(1,3,11,41,157,607,2367,9277)$	$\frac{5z-1+\sqrt{1-2z-7z^2}}{4z(1-4z)}$	$\frac{1}{4\pi}\frac{\sqrt{7+2t-t^2}}{4-t}$	$[1-2\sqrt{2}, 1+2\sqrt{2}]$
A151323  $(1,3,14,67,342,1790,9580)$	$\frac{\sqrt[4]{\frac{1+2z}{1-6z}}-1}{2z}$	$\frac{1}{2\sqrt{2}\pi}\sqrt[4]{\frac{2+t}{6-t}}$	$[-2, 6]$

A SIAM Review combinatorial identity

Problem 87-8, *by* JOHN W. MOON (University of Alberta).

Show that

$$\sum_{n=1}^{\infty} \frac{56n^2+33n-8}{(n+2)(n+1)} f_n^2 = 1$$

where

$$f_n = \frac{4^{-n}}{n}\binom{2n-2}{n-1} \quad \text{for } n \geqq 1.$$

Background. A *branch* of a rooted tree T_n is a maximal subtree that does not contain the root. A branch B with i nodes is a *primary* branch of T_n if $n/2 \leqq i \leqq n-1$; if T_n has a primary branch B with i nodes, then a branch C with j nodes is a *secondary* branch if $(n-i)/2 \leqq j \leqq n-1-i$. For many families F of rooted trees, the fraction of trees T_n in F that have a primary branch tends to 1 as $n \to \infty$. (See A. Meir and J.W. Moon, *On major and minor branches of rooted trees*, Canad. J. Math., 39 (1987) 673-693). It can be shown that the fraction of plane trees T_n that have a secondary branch tends to a limit p as $n \to \infty$, where

$$p = 3 - 12 \sum_{n=1}^{\infty} \frac{13n^2+5n-2}{(n+1)(n+2)} f_n^2.$$

If we appeal to the proposed identity then we obtain the more rapidly converging expression

$$p = \frac{3}{14} + \frac{3}{14} \sum_{n=1}^{\infty} \frac{149n+8}{(n+1)(n+2)} f_n^2$$

from which we find that $p = .59 \cdots$.

- Computer algebra conjectures and proves $p = \frac{28}{15\pi}$.

Monthly (AMM) problems with a combinatorial flavor that can be solved using computer algebra

Expansion of a Symmetric Determinant

E 2297 [1971, 543]. *Proposed by Richard Stanley, Harvard University*

Let $L(n)$ be the total number of distinct monomials appearing in the expansion of the determinant of an $n \times n$ symmetric matrix $A = (a_{ij})$. For instance, $L(3) = 5$. Show that

$$\sum_{n=0}^{\infty} L(n)x^n/n! = (1-x)^{-1/2} \exp(\tfrac{1}{2}x + \tfrac{1}{4}x^2),$$

where $|x| < 1$, and where we define $L(0) = 1$.

Units of Chains

6342 [1981, 294]. *Proposed by Richard Stanley, Massachusetts Institute of Technology.*

Let $f(n)$ be the number of nonisomorphic n-element partially ordered sets P which do not contain three pairwise incomparable elements. (Equivalently, P is a union of two chains.) Let

$$F(x) = 1 + \sum_{n \geq 1} f(n)x^n = 1 + x + 2x^2 + 4x^3 + 10x^4 + \cdots.$$

Show that

$$F(x) = \frac{4}{2 - 2x + \sqrt{1-4x} + \sqrt{1-4x^2}}.$$

Noncrossing Trees

E 3170 [1986, 650]. *Proposed by The Howard University Group, Washington, D.C.*

Construct a graph as follows: Put $n + 1$ labeled vertices around a circle and let the edges be the straight line segments connecting any two vertices. A tree is noncrossing if no two edges intersect except at the vertices. Enumerate the number of noncrossing spanning trees for this graph. For $n = 1, 2, 3$, the numbers are 1, 3, 12, respectively.

An Unexpected Appearance of the Catalan Numbers

10905 [2001, 871]. *Proposed by Richard P. Stanley, Massachusetts Institute of Technology, Cambridge, MA.* Let $f(n) = \sum_P (-1)^{w(P)}$, where P ranges over all lattice paths in the plane with $2n$ steps, starting and ending at the origin, with steps $(1,0)$, $(0,1)$, $(-1,0)$, $(0,-1)$, and where $w(P)$ denotes the winding number of P with respect to the point $(1/2, 1/2)$. Show that $f(n) = 4^n C_n$, where $C_n = \binom{2n}{n} \Big/ (n+1)$, the nth Catalan number.

Three-dimensional Lattice Walks in the Upper Half-Space

10795 [2000, 367]. *Proposed by Emeric Deutsch, Polytechnic University, Brooklyn, NY.* A *3-dimensional lattice walk* of length n takes n successive unit steps, each in one of the six coordinate directions. How many 3-dimensional lattice walks of length n are there that begin at the origin and never go below the horizontal plane?

Another Type of Lattice Path

10658 [1998, 366]. *Proposed by Emeric Deutsch, Polytechnic University, Brooklyn, NY.* Consider walks on the integer lattice in the plane that start at $(0, 0)$, that stay in the first quadrant (they may touch the x-axis), and such that each step is either $(2, 1)$, $(1, 2)$, or $(1, -1)$. For each nonnegative integer n, how many paths are there to $(3n, 0)$?

The First Third

6637 [1990, 621]. *Proposed by Herbert S. Wilf, University of Pennsylvania, Philadelphia, PA.*

Let $f(n)$ be the sum of the first one-third of the coefficients in the expansion of $(1+x)^{3n}$, i.e.,

$$f(n) = \sum_{k=0}^{n} \binom{3n}{k} \qquad (n = 0, 1, 2, \ldots).$$

Prove that

$$\sum_{n=0}^{\infty} f(n)\left(\frac{4u^2}{27}\right)^n = \frac{u}{u - 2\sin(\frac{1}{3}\arcsin u)} - \frac{2u}{2u - 3\sin(\frac{1}{3}\arcsin u)}.$$

11501. *Proposed by Finbarr Holland, University College Cork, Cork, Ireland.* (Correction) Let

$$g(z) = 1 - \frac{3}{\frac{1}{1-az} + \frac{1}{1-iz} + \frac{1}{1+iz}}.$$

Show that the coefficients in the Taylor series expansion of g about 0 are all nonnegative if and only if $a \geq \sqrt{3}$.

11567. *Proposed by David Callan, University of Wisconsin-Madison, Madison, WI.* How many arrangements $(a_1, \ldots, a_{2n})$ of the multiset $\{1, 1, 2, 2, \ldots, n, n\}$ satisfy the following two conditions: (i) All entries between the two occurrences of any given value i exceed i, and (ii) No three entries increase from left to right with the last two adjacent? (When $n = 3$, one such arrangement is 122133.)

11573. *Proposed by Rob Pratt, SAS Institute, Cary, NC.* A *Sudoku permutation matrix* (SPM) of order n^2 is a permutation matrix of order n^2 with exactly one 1 in each of the n^2 submatrices of order n obtained by partitioning the original matrix into an n-by-n array of submatrices. Thus, for $n = 2$, the permutation 1324 yields an SPM, but the identity permutation 1234 does not. Find the number of SPMs of order n^2.

11610. *Proposed by Richard P. Stanley, Massachussetts Institute of Technology, Cambridge, MA.* Let $f(n)$ be the number of binary words $a_1 \cdots a_n$ of length n that have the same number of pairs $a_i a_{i+1}$ equal to 00 as equal to 01. Show that

$$\sum_{n=0}^{\infty} f(n)t^n = \frac{1}{2}\left(\frac{1}{1-t} + \frac{1+2t}{\sqrt{(1-t)(1-2t)(1+t+2t^2)}}\right).$$

- Last one as an exercise tomorrow.

A money changing problem

Question[†]: The number of ways one can change any amount of banknotes of $10\,€, 20\,€, \ldots$ using coins of 50 cents, $1\,€$ and $2\,€$ is always a perfect square.

[†]Free adaptation of Pb. 1, Ch. 1, p. 1, vol. 1 of Pólya and Szegö's Problems Book (1925)

This is equivalent to finding the number M_{20k} of solutions $(a, b, c) \in \mathbb{N}^3$ of

$$a + 2b + 4c = 20k.$$

Euler-Comtet's denumerants: $\displaystyle\sum_{n\geq 0} M_n x^n = \frac{1}{(1-x)(1-x^2)(1-x^4)}.$

```
> f:=1/(1-x)/(1-x^2)/(1-x^4):
> S:=series(f,x,201):
> [seq(coeff(S,x,20*k),k=1..10)];
```

```
[36, 121, 256, 441, 676, 961, 1296, 1681, 2116, 2601]
```

```
> subs(n=20*k,gfun[ratpolytocoeff](f,x,n)):
```

$$\frac{17}{32} + \frac{(20k+1)(20k+2)}{16} + 5k + \frac{(-1)^{-20k}(20k+1)}{16} + \frac{5(-1)^{-20k}}{32} + \sum_{\alpha^2+1=0}\left(-\frac{(\frac{1}{16} - \frac{1}{16}\alpha)\alpha^{-20k}}{\alpha}\right)$$

```
> value(subs(_alpha^(-20*k)=1,%)):
> simplify(%) assuming k::posint:
> factor(%);
```

```
                    2
           (5 k + 1)
```

INTRODUCTION

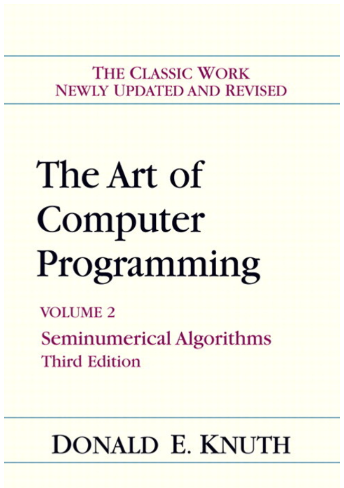
2. Computer Algebra

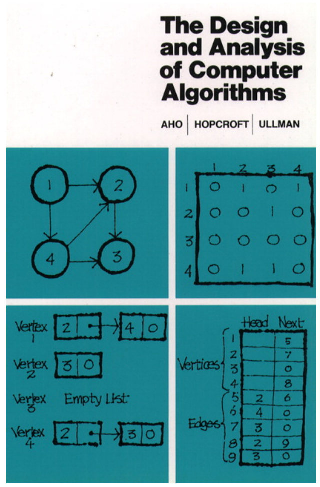
General framework

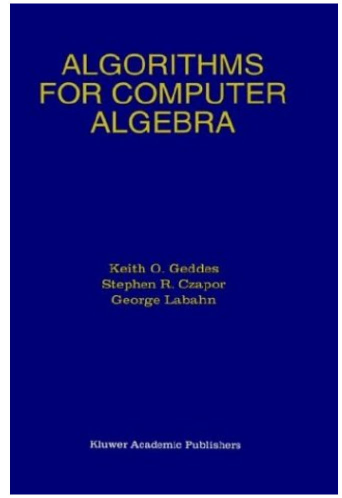
$$\mathsf{Computeralgebra} = \mathsf{effectivemathematics}and\mathsf{algebraiccomplexity}$$

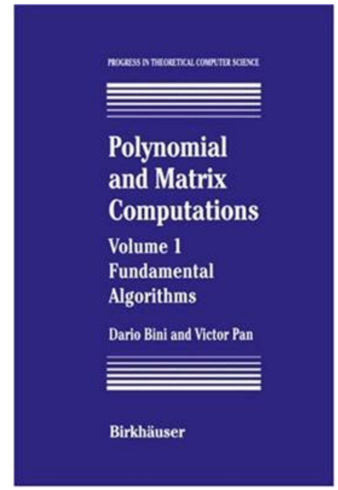
- Effective mathematics: what can we compute?
- their complexity: how fast?

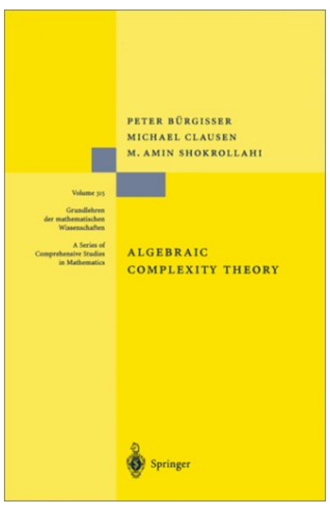
Computer algebra books

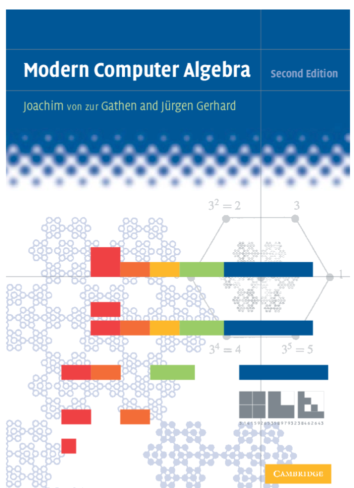


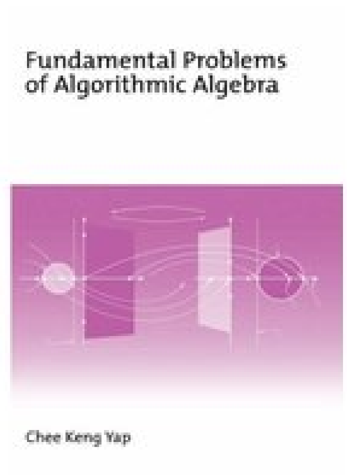


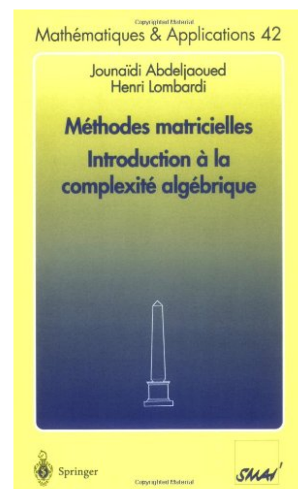












Mathematical Objects

- Main objects
  - integers $\mathbb{Z}$
  - polynomials $\mathbb{K}[x]$
  - rational functions $\mathbb{K}(x)$
  - power series $\mathbb{K}[[x]]$
  - matrices $\mathcal{M}_r(\mathbb{K})$
  - linear recurrences with constant, or polynomial, coefficients $\mathbb{K}[n]\langle S_n\rangle$
  - linear differential equations with polynomial coefficients $\mathbb{K}[x]\langle \partial_x\rangle$

  where $\mathbb{K}$ is a field (generally supposed of characteristic 0 or large)

- Secondary/auxiliary objects
  - polynomial matrices $\mathcal{M}_r(\mathbb{K}[x])$
  - power series matrices $\mathcal{M}_r(\mathbb{K}[[x]])$

Overview

Today

1. Introduction
2. High Precision Approximations
   - Fast multiplication, binary splitting, Newton iteration
3. Tools for Conjectures
   - Hermite-Padé approximants, p-curvature

Tomorrow morning

4. Tools for Proofs
   - Symbolic method, resultants, D-finiteness, creative telescoping

Tomorrow night

- Exercises with Maple

HIGH PRECISION

1. Fast Multiplication

Complexity yardsticks

Important features:

- addition is easy: naive algorithm already optimal
- multiplication is the most basic (non-trivial) problem
- almost all problems can be reduced to multiplication

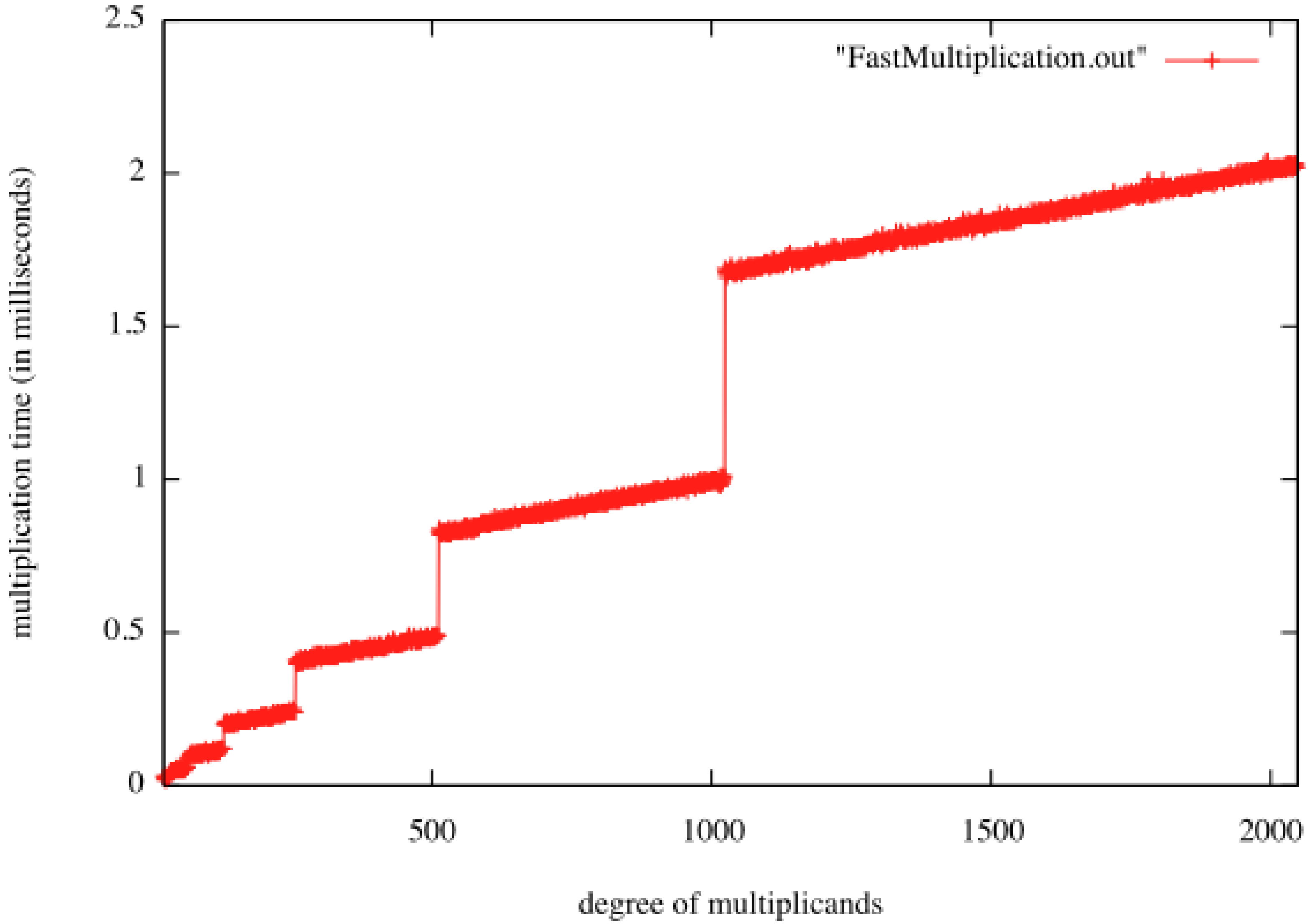
Are there quasi-optimal algorithms for:

- integer/polynomial/power series multiplication? Yes!
- matrix multiplication? Big open problem!

Complexity yardsticks

$$
\begin{array}{rcl}
\mathsf{M}(n) & = & \text{complexity of } \textsf{multiplication} \text{ in } \mathbb{K}[x]_{<n}, \text{ and of } n\text{-bit integers} \\
& = & O(n^2) \ \text{ by the naive algorithm} \\
& = & O\big(n^{1.58}\big) \ \text{ by } \textsf{Karatsuba}\text{'s algorithm} \\
& = & O\big(n^{\log_\alpha(2\alpha-1)}\big) \ \text{ by the } \textsf{Toom-Cook} \text{ algorithm } (\alpha \geq 3) \\
& = & O\big(n \log n \operatorname{loglog} n\big) \ \text{ by the } \textsf{Schönhage-Strassen} \text{ algorithm} \\
\\
\mathsf{MM}(r) & = & \text{complexity of } \textsf{matrix product} \text{ in } \mathcal{M}_r(\mathbb{K}) \\
& = & O(r^3) \ \text{ by the naive algorithm} \\
& = & O(r^{2.81}) \ \text{ by } \textsf{Strassen}\text{'s algorithm} \\
& = & O(r^{2.38}) \ \text{ by the } \textsf{Coppersmith-Winograd} \text{ algorithm} \\
\\
\mathsf{MM}(r,n) & = & \text{complexity of } \textsf{polynomial matrix product} \text{ in } \mathcal{M}_r(\mathbb{K}[x]_{<n}) \\
& = & O(r^3\, \mathsf{M}(n)) \ \text{ by the naive algorithm} \\
& = & O(\mathsf{MM}(r)\, n \log(n) + r^2 n \log n \operatorname{loglog} n) \ \text{ by the } \textsf{Cantor-Kaltofen} \text{ algo} \\
& = & O(\mathsf{MM}(r)\, n + r^2\, \mathsf{M}(n)) \ \text{ by the } \textsf{B-Schost} \text{ algorithm}
\end{array}
$$

Fast polynomial multiplication in practice



Practical complexity of Magma's multiplication in $\mathbb{F}_p[x]$, for $p = 29 \times 2^{57} + 1$.

What can be computed in 1 minute with a CA system*

polynomial product† in degree 14,000,000 (>1 year with schoolbook)

product of two integers with 500,000,000 binary digits

factorial of $N = 20,000,000$ (output of 140,000,000 digits)

gcd of two polynomials of degree 600,000

resultant of two polynomials of degree 40,000

factorization of a univariate polynomial of degree 4,000

factorization of a bivariate polynomial of total degree 500

resultant of two bivariate polynomials of total degree 100 (output 10,000)

product/sum of two algebraic numbers of degree 450 (output 200,000)

determinant (char. polynomial) of a matrix with 4,500 (2,000) rows

determinant of an integer matrix with 32-bit entries and 700 rows

---

*on a PC, (Intel Xeon X5160, 3GHz processor, with 8GB RAM), running Magma V2.16-7

†in $\mathbb{K}[x]$, for $\mathbb{K} = \mathbb{F}_{67108879}$

Discrete Fourier Transform

[Gauss 1866, Cooley-Tukey 1965]

DFT Problem: Given $n = 2^k$, $f \in \mathbb{K}[x]_{<n}$, and $\omega \in \mathbb{K}$ a primitive n-th root of unity, compute $(f(1), f(\omega), \ldots, f(\omega^{n-1}))$

Idea: Write $f = f_{\text{even}}(x^2) + x f_{\text{odd}}(x^2), \quad$ with $\deg(f_{\text{even}}), \deg(f_{\text{odd}}) < n/2$.

Then $f(\omega^j) = f_{\text{even}}(\omega^{2j}) + \omega^j f_{\text{odd}}(\omega^{2j})$, and $(\omega^{2j})_{0 \le j < n} = \frac{n}{2}$-roots of 1.

Complexity: $\quad \mathsf{F}(n) = 2 \cdot \mathsf{F}(n/2) + O(n) \quad \Longrightarrow \quad \mathsf{F}(n) = O(n \log n)$

Inverse DFT

IDFT Problem: Given $n = 2^k$, $v_0, \ldots, v_{n-1} \in \mathbb{K}$ and $\omega \in \mathbb{K}$ a primitive n-th root of unity, compute $f \in \mathbb{K}[x]_{<n}$ such that $f(1) = v_0, \ldots, f(\omega^{n-1}) = v_{n-1}$

- $V_\omega \cdot V_{\omega^{-1}} = n \cdot I_n \;\rightarrow\;$ performing the inverse DFT in size n amounts to:
  - performing a DFT at
$$\frac{1}{1}, \quad \frac{1}{\omega}, \quad \ldots, \quad \frac{1}{\omega^{n-1}}$$
  - dividing the results by n.
- this new DFT is the same as before:
$$\frac{1}{\omega^i} = \omega^{n-i},$$
  so the outputs are just shuffled.

Consequence: the cost of the inverse DFT is $O(n \log(n))$

FFT polynomial multiplication

Suppose the basefield $\mathbb{K}$ contains enough roots of unity

To multiply two polynomials f, g in $\mathbb{K}[x]$, of degrees $< n$:

- find $N = 2^k$ such that $h = fg$ has degree less than N — $N \leq 4n$
- compute DFT(f, N) and DFT(g, N) — $O(N \log(N))$
- multiply pointwise these values to get DFT(h, N) — $O(N)$
- recover h by inverse DFT — $O(N \log(N))$

Complexity: $O(N \log(N)) = O(n \log(n))$

General case: Create artificial roots of unity — $O(n \log(n) \log \log n)$

HIGH PRECISION

2. Binary Splitting

Example: fast factorial

Problem: Compute $N! = 1 \times \cdots \times N$

Naive iterative way: unbalanced multiplicands $\tilde{O}(N^2)$

- Binary Splitting: balance computation sequence so as to take advantage of fast multiplication (operands of same sizes):

$$N! = \underbrace{(1 \times \cdots \times \lfloor N/2 \rfloor)}_{\text{size } \frac{1}{2} N \log N} \times \underbrace{((\lfloor N/2 \rfloor + 1) \times \cdots \times N)}_{\text{size } \frac{1}{2} N \log N}$$

  and recurse. Complexity $\tilde{O}(N)$.

- Extends to matrix factorials $A(N)A(N-1)\cdots A(1)$ $\tilde{O}(N)$
  $\longrightarrow$ recurrences of arbitrary order.

Application to recurrences

Problem: Compute the N-th term u_N of a P-recursive sequence

$$p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0, \qquad (n \in \mathbb{N})$$

Naive algorithm: unroll the recurrence $\tilde{O}(N^2)$ bit ops.

Binary splitting: $U_n = (u_n, \ldots, u_{n+r-1})^T$ satisfies the 1st order recurrence

$$U_{n+1} = \frac{1}{p_r(n)} A(n) U_n \quad \text{with} \quad A(n) = \begin{bmatrix} & p_r(n) & & \\ & & \ddots & \\ & & & p_r(n) \\ -p_0(n) & -p_1(n) & \ldots & -p_{r-1}(n) \end{bmatrix}.$$

$\Longrightarrow u_N$ reads off the matrix factorial $A(N-1)\cdots A(0)$

[Chudnovsky-Chudnovsky, 1987]: Binary splitting strategy $\tilde{O}(N)$ bit ops.

Application: fast computation of $e = \exp(1)$

[Brent 1976]

$$e_n = \sum_{k=0}^{n} \frac{1}{k!} \quad \longrightarrow \quad \exp(1) = 2.7182818284590452\ldots$$

Recurrence $e_n - e_{n-1} = 1/n! \iff n(e_n - e_{n-1}) = e_{n-1} - e_{n-2}$ rewrites

$$\begin{bmatrix} e_{N-1} \\ e_N \end{bmatrix} = \frac{1}{N} \underbrace{\begin{bmatrix} 0 & N \\ -1 & N+1 \end{bmatrix}}_{C(N)} \begin{bmatrix} e_{N-2} \\ e_{N-1} \end{bmatrix} = \frac{1}{N!} C(N)C(N-1)\cdots C(1) \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

- e_N in $\tilde{O}(N)$ bit operations [Brent 1976]
- generalizes to the evaluation of any D-finite series at an algebraic number [Chudnovsky-Chudnovsky 1987] $\tilde{O}(N)$ bit ops.

Implementation in gfun

[Mezzarobba, S. 2010]

```
> rec:={n*(e(n) - e(n-1)) = e(n-1) - e(n-2), e(0)=1, e(1)=2};
> pro:=rectoproc(rec,e(n));
```

```
pro := proc(n::nonnegint)
local i1, loc0, loc1, loc2, tmp2, tmp1, i2;
    if n <= 22 then
        loc0 := 1;
        loc1 := 2;
        if n = 0 then return loc0
        else for i1 to n - 1 do
                loc2 := (-loc0 + loc1 + loc1*(i1 + 1))/(i1 + 1); loc0 := loc1; loc1 := loc2
            end do
        end if; loc1
    else
        tmp1 := `gfun/rectoproc/binsplit`([
            'ndmatrix'(Matrix([[0, i2 + 2], [-1, i2 + 3]]), i2 + 2), i2, 0, n,
            matrix_ring(ad, pr, ze, ndmatrix(Matrix(2, 2, [[...],[...]],
            datatype = anything, storage = empty, shape = [identity]), 1)),
            expected_entry_size], Vector(2, [...], datatype = anything));
        tmp1 := subs({e(0) = 1, e(1) = 2}, tmp1);  tmp1
    end if
end proc
```

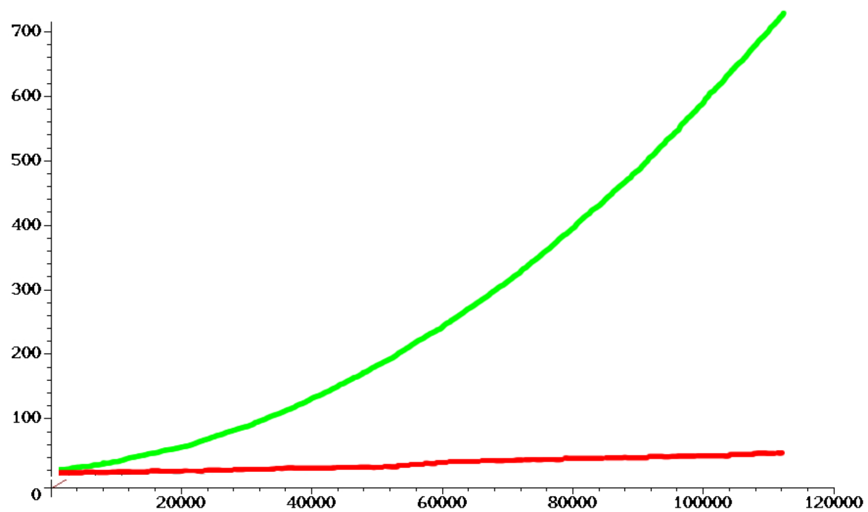
```
> tt:=time(): x:=pro(50000): time()-tt, evalf(x-exp(1), 200000);
```

```
1.827, 0.
```

Application: record computation of π

[Chudnovsky-Chudnovsky 1987] fast convergence hypergeometric identity

$$\frac{1}{\pi} = \frac{1}{53360\sqrt{640320}} \sum_{n\geq 0} \frac{(-1)^n (6n)!(13591409 + 545140134n)}{n!^3(3n)!(8 \cdot 100100025 \cdot 327843840)^n}.$$



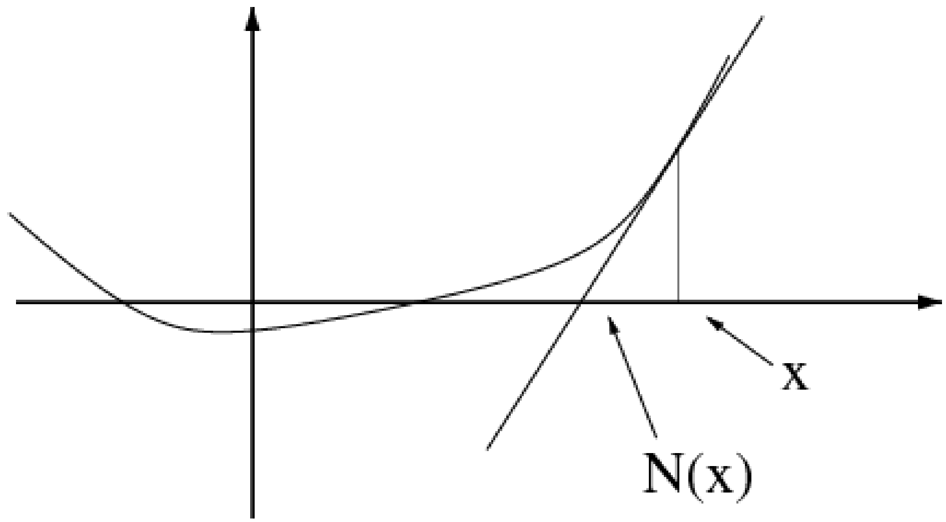
- Used in Maple & Mathematica: 1st order recurrence, yields 14 correct digits per iteration $\longrightarrow$ 4 billion digits [Chudnovsky-Chudnovsky 1994]
- Current record on a PC: 10000 billion digits [Kondo & Yee 2011]

HIGH PRECISION

3. Newton Iteration

Newton's tangent method: real case

[Newton, 1671]



$$x_{\kappa+1} = \mathcal{N}(x_\kappa) = x_\kappa - (x_\kappa^2 - 2)/(2x_\kappa), \quad x_0 = 1$$

$$x_1 = 1.50000000000000000000000000000000$$

$$x_2 = 1.41666666666666666666666666666667$$

$$x_3 = 1.41421568627450980392156862745098$$

$$x_4 = 1.41421356237468991062629557889015$$

$$x_5 = 1.41421356237309504880168962350253$$

Newton's tangent method: power series case

$$x_{\kappa+1} = \mathcal{N}(x_\kappa) = x_\kappa - (x_\kappa^2 - (1-t))/(2x_\kappa), \quad x_0 = 1$$

$$x_1 = 1 - \frac{1}{2}t$$

$$x_2 = 1 - \frac{1}{2}t - \frac{1}{8}t^2 - \frac{1}{16}t^3 - \frac{1}{32}t^4 - \frac{1}{64}t^5 - \frac{1}{128}t^6 - \frac{1}{256}t^7 - \frac{1}{512}t^8 - \frac{1}{1024}t^9 + \cdots$$

$$x_3 = 1 - \frac{1}{2}t - \frac{1}{8}t^2 - \frac{1}{16}t^3 - \frac{5}{128}t^4 - \frac{7}{256}t^5 - \frac{21}{1024}t^6 - \frac{33}{2048}t^7 - \frac{107}{8192}t^8 - \frac{177}{16384}t$$

Newton's tangent method: power series case

In order to solve $\varphi(x, g) = 0$ in $\mathbb{K}[[x]]$ (where $\varphi \in \mathbb{K}[[x, y]]$, $\varphi(0, 0) = 0$ and $\varphi_y(0, 0) \neq 0$), iterate

$$g_{\kappa+1} = g_\kappa - \frac{\varphi(g_\kappa)}{\varphi_y(g_\kappa)} \mod x^{2^{\kappa+1}}$$

$$g - g_{\kappa+1} = g - g_\kappa + \frac{\varphi(g) + (g_\kappa - g)\varphi_y(g) + O((g - g_\kappa)^2)}{\varphi_y(g) + O(g - g_\kappa)} = O((g - g_\kappa)^2).$$

- The number of correct coefficients doubles after each iteration
- Total cost $= \mathbf{2} \times \Big($ the cost of the last iteration $\Big)$

Theorem [Cook 1966, Sieveking 1972 & Kung 1974, Brent 1975]
Division, logarithm and exponential of power series in $\mathbb{K}[[x]]$ can be computed at precision N using $O(\mathsf{M}(N))$ operations in $\mathbb{K}$

Division, logarithm and exponential of power series

[Sieveking1972, Kung1974, Brent1975]

To compute the reciprocal of $f \in \mathbb{K}[[x]]$ with $f(0) \neq 0$, choose $\varphi(g) = 1/g - f$:

$$g_0 = 1/f_0 \quad \text{and} \quad g_{\kappa+1} = g_\kappa + g_\kappa(1 - f g_\kappa) \mod x^{2^{\kappa+1}} \quad \text{for } \kappa \geq 0.$$

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \implies \mathsf{C}(N) = O(\mathsf{M}(N))$

Corollary: division of power series at precision N in $O(\mathsf{M}(N))$

Division, logarithm and exponential of power series

[Sieveking1972, Kung1974, Brent1975]

To compute the reciprocal of $f \in \mathbb{K}[[x]]$, choose $\varphi(g) = 1/g - f$:

$$g_0 = 1/f_0 \quad \text{and} \quad g_{\kappa+1} = g_\kappa + g_\kappa(1 - f g_\kappa) \mod x^{2^{\kappa+1}} \quad \text{for } \kappa \geq 0.$$

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \implies \mathsf{C}(N) = O(\mathsf{M}(N))$

Corollary: division of power series at precision N in $O(\mathsf{M}(N))$

Corollary: Logarithm $\log(f) = -\sum_{i\geq 1} \frac{(1-f)^i}{i}$ of $f \in 1 + x\mathbb{K}[[x]]$ in $O(\mathsf{M}(N))$:

- compute the Taylor expansion of $h = f'/f$ modulo x^{N-1} $O(\mathsf{M}(N))$
- take the antiderivative of h $O(N)$

Division, logarithm and exponential of power series

[Sieveking1972, Kung1974, Brent1975]

To compute the reciprocal of $f \in \mathbb{K}[[x]]$, choose $\varphi(g) = 1/g - f$:

$$g_0 = 1/f_0 \quad \text{and} \quad g_{\kappa+1} = g_\kappa + g_\kappa(1 - f g_\kappa) \quad \mod x^{2^{\kappa+1}} \qquad \text{for } \kappa \geq 0.$$

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \qquad \Longrightarrow \qquad \mathsf{C}(N) = O(\mathsf{M}(N))$

Corollary: division of power series at precision N in $O(\mathsf{M}(N))$

Corollary: Logarithm $\log(f) = -\sum_{i \geq 1} \frac{(1-f)^i}{i}$ of $f \in 1 + x\mathbb{K}[[x]]$ in $O(\mathsf{M}(N))$:

- compute the Taylor expansion of $h = f'/f$ modulo x^{N-1} $\qquad O(\mathsf{M}(N))$
- take the antiderivative of h $\qquad O(N)$

Corollary: Exponential $\exp(f) = \sum_{i \geq 0} \frac{f^i}{i!}$ of $f \in x\mathbb{K}[[x]]$. Use $\phi(g) = \log(g) - f$:

$$g_0 = 1 \quad \text{and} \quad g_{\kappa+1} = g_\kappa - g_\kappa\left(\log(g_\kappa) - f\right) \quad \mod x^{2^{\kappa+1}} \qquad \text{for } \kappa \geq 0.$$

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \qquad \Longrightarrow \qquad \mathsf{C}(N) = O(\mathsf{M}(N))$

Application: Euclidean division for polynomials

[Strassen, 1973]

Pb: Given $F, G \in \mathbb{K}[x]_{\leq N}$, compute (Q, R) in Euclidean division $F = QG + R$

Naive algorithm: $O(N^2)$

Idea: look at $F = QG + R$ from infinity: $Q \sim_{+\infty} F/G$

Let $N = \deg(F)$ and $n = \deg(G)$. Then $\deg(Q) = N - n$, $\deg(R) < n$ and

$$\underbrace{F(1/x)x^N}_{\mathrm{rev}(F)} = \underbrace{G(1/x)x^n}_{\mathrm{rev}(G)} \cdot \underbrace{Q(1/x)x^{N-n}}_{\mathrm{rev}(Q)} + \underbrace{R(1/x)x^{\deg(R)}}_{\mathrm{rev}(R)} \cdot x^{N-\deg(R)}$$

Algorithm:

- Compute $\mathrm{rev}(Q) = \mathrm{rev}(F)/\mathrm{rev}(G) \mod x^{N-n+1}$ $\quad O(\mathsf{M}(N))$
- Recover Q $\quad O(N)$
- Deduce $R = F - QG$ $\quad O(\mathsf{M}(N))$

Application: conversion coefficients $\leftrightarrow$ power sums

[Schönhage, 1982]

Any polynomial $F = x^n + a_1 x^{n-1} + \cdots + a_n$ in $\mathbb{K}[x]$ can be represented by its first n power sums $S_i = \sum_{F(\alpha)=0} \alpha^i$

Conversions coefficients $\leftrightarrow$ power sums can be performed

- either in $O(n^2)$ using Newton identities (naive way):

$$i a_i + S_1 a_{i-1} + \cdots + S_i = 0, \quad 1 \leq i \leq n$$

- or in $O(\mathsf{M}(n))$ using generating series

$$\frac{\mathsf{rev}(F)'}{\mathsf{rev}(F)} = -\sum_{i\geq 0} S_{i+1} x^i \quad \Longleftrightarrow \quad \mathsf{rev}(F) = \exp\left(-\sum_{i\geq 1} \frac{S_i}{i} x^i\right)$$

Application: special bivariate resultants

[B-Flajolet-S-Schost, 2006]

Composed products and sums: manipulation of algebraic numbers

$$F \otimes G = \prod_{F(\alpha)=0, G(\beta)=0} (x - \alpha\beta), \quad F \oplus G = \prod_{F(\alpha)=0, G(\beta)=0} (x - (\alpha + \beta))$$

Output size: $N = \deg(F)\deg(G)$

Linear algebra: χ_{xy}, χ_{x+y} in $\mathbb{K}[x,y]/(F(x), G(y))$ $O(\mathsf{MM}(N))$

Resultants: $\mathrm{Res}_y\left(F(y), y^{\deg(G)}G(x/y)\right), \mathrm{Res}_y\left(F(y), G(x-y)\right)$ $O(N^{1.5})$

Better: $\otimes$ and $\oplus$ are easy in Newton representation $O(\mathsf{M}(N))$

$$\sum \alpha^s \sum \beta^s = \sum (\alpha\beta)^s \qquad \text{and}$$

$$\sum \frac{\sum(\alpha+\beta)^s}{s!} x^s = \left(\sum \frac{\sum \alpha^s}{s!} x^s\right) \left(\sum \frac{\sum \beta^s}{s!} x^s\right)$$

Corollary: Fast polynomial shift $P(x+a) = P(x) \oplus (x+a)$ $O(\mathsf{M}(\deg(P)))$

Newton iteration on power series: operators and systems

In order to solve an equation $\phi(Y) = 0$, with $\phi : (\mathbb{K}[[x]])^r \to (\mathbb{K}[[x]])^r$,

1. Linearize: $\phi(Y_\kappa - U) = \phi(Y_\kappa) - D\phi|_{Y_\kappa} \cdot U + O(U^2)$,
   where $D\phi|_Y$ is the differential of ϕ at Y.
2. Iterate: $Y_{\kappa+1} = Y_\kappa - U_{\kappa+1}$, where $U_{\kappa+1}$ is found by
3. Solve linear equation: $D\phi|_{Y_k} \cdot U = \phi(Y_\kappa)$ with $\operatorname{val} U > 0$.

Then, the sequence Y_κ converges quadratically to the solution Y.

Application: inversion of power series matrices

[Schulz, 1933]

To compute the inverse Z of a matrix of power series $Y \in \mathcal{M}_r(\mathbb{K}[[x]])$:

- Choose the map $\phi : Z \mapsto I - YZ$ with differential $D\phi|_Y : U \mapsto -YU$
- Equation for U: $-YU = I - YZ_\kappa \mod x^{2^{\kappa+1}}$
- Solution: $U = -Y^{-1}(I - YZ_\kappa) = -Z_\kappa(I - YZ_\kappa) \bmod x^{2^{\kappa+1}}$

This yields the following Newton-type iteration for Y^{-1}

$$Z_{\kappa+1} = Z_\kappa + Z_\kappa(I_r - YZ_\kappa) \mod x^{2^{\kappa+1}}$$

Complexity:

$\mathsf{C}_{\mathrm{inv}}(N) = \mathsf{C}_{\mathrm{inv}}(N/2) + O(\mathsf{MM}(r, N)) \quad \Longrightarrow \quad \mathsf{C}_{\mathrm{inv}}(N) = O(\mathsf{MM}(r, N))$

Application: non-linear systems

In order to solve a system $Y = H(Y) = \phi(Y) + Y$, with $H : (\mathbb{K}[[x]])^r \to (\mathbb{K}[[x]])^r$, such that $I_r - \partial H/\partial Y$ is invertible at 0.

1. Linearize: $\phi(Y_\kappa - U) - \phi(Y_\kappa) = U - \partial H/\partial Y(Y_\kappa) \cdot U + O(U^2)$.
2. Iterate $Y_{\kappa+1} = Y_\kappa - U_{\kappa+1}$, where $U_{\kappa+1}$ is found by
3. Solve linear equation: $(I_r - \partial H/\partial Y(Y_\kappa)) \cdot U = H(Y_\kappa) - Y_\kappa$ with $\operatorname{val} U > 0$.

This yields the following Newton-type iteration:

$$\begin{cases} Z_{\kappa+1} & = Z_\kappa + Z_\kappa(I_r - (I_r - \partial H/\partial Y(Y_\kappa))Z_\kappa) \mod x^{2^{\kappa+1}} \\ Y_{\kappa+1} & = Y_\kappa - Z_{\kappa+1}(H(Y_\kappa) - Y_\kappa) \mod x^{2^{\kappa+1}} \end{cases}$$

computing simultaneously a matrix and a vector.

Example: Mappings

```
> mappings:={M=Set(Cycle(Tree)),Tree=Prod(Z,Set(Tree))}:
> combstruct[gfeqns](mappings,labeled,x);
```

$$\left[M(x) = \frac{1}{1 - \mathit{Tree}(x)}, \quad \mathit{Tree}(x) = x \exp(\mathit{Tree}(x))\right]$$

```
> countmappings:=SeriesNewtonIteration(mappings,labelled,x):
> countmappings(10);
```

$$\Bigg[M = 1 + x + 2\,x^2 + \frac{9}{2}x^3 + \frac{32}{3}x^4 + \frac{625}{24}x^5 + \frac{324}{5}x^6 + \frac{117649}{720}x^7 + \frac{131072}{315}x^8 + \frac{4782969}{4480}x^9 + O\left(x^{10}\right),$$
$$\mathit{Tree} = x + x^2 + \frac{3}{2}x^3 + \frac{8}{3}x^4 + \frac{125}{24}x^5 + \frac{54}{5}x^6 + \frac{16807}{720}x^7 + \frac{16384}{315}x^8 + \frac{531441}{4480}x^9 + O\left(x^{10}\right)\Bigg]$$

Code Pivoteau-S-Soria, should end up in `combstruct`

Application: quasi-exponential of power series matrices

[B-Chyzak-Ollivier-Salvy-Schost-Sedoglavic 2007]

To compute the solution $Y \in \mathcal{M}_r(\mathbb{K}[[x]])$ of the system $Y' = AY$

- choose the map $\phi : Y \mapsto Y' - AY$, with differential ϕ.
- the equation for U is $\quad U' - AU = Y_\kappa' - AY_\kappa \mod x^{2^{\kappa+1}}$
- the method of variation of constants yields the solution $U = Y_\kappa V_\kappa \mod x^{2^{\kappa+1}},\;\; Y_\kappa' - AY_\kappa = Y_\kappa V_\kappa' \mod x^{2^{\kappa+1}}$

This yields the following Newton-type iteration for Y:

$$Y_{\kappa+1} = Y_\kappa - Y_\kappa \int Y_\kappa^{-1} \left(Y_\kappa' - AY_\kappa\right) \quad \mod x^{2^{\kappa+1}}$$

Complexity:

$\mathsf{C}_{\text{solve}}(N) = \mathsf{C}_{\text{solve}}(N/2) + O(\mathsf{MM}(r,N)) \qquad \Longrightarrow \qquad \mathsf{C}_{\text{solve}}(N) = O(\mathsf{MM}(r,N))$

TOOLS FOR CONJECTURES

1. Hermite-Padé Approximants

Definition

Definition: Given a column vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and an n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, a Hermite-Padé approximant of type $\mathbf{d}$ for $\mathbf{F}$ is a row vector $\mathbf{P} = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n$, ($\mathbf{P} \neq 0$), such that:

(1) $\mathbf{P} \cdot \mathbf{F} = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma)$ with $\sigma = \sum_i (d_i + 1) - 1$,

(2) $\deg(P_i) \leq d_i$ for all i.

σ is called the order of the approximant $\mathbf{P}$.

- Very useful concept in number theory (transcendence theory):
  - [Hermite, 1873]: e is transcendent.
  - [Lindemann, 1882]: π is transcendent, and so does e^α for any $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$.
  - [Beukers, 1981]: reformulate Apéry's proof that $\zeta(3) = \sum_n \frac{1}{n^3}$ is irrational.
  - [Rivoal, 2000]: there exist an infinite number of k such that $\zeta(2k+1) \notin \mathbb{Q}$.

Worked example

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1,C,C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + 42x^5 + O(x^6)$.

This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ such that

$$\alpha_0+\alpha_1 x+(\beta_0+\beta_1 x)(1+x+2x^2+5x^3+14x^4)+(\gamma_0+\gamma_1 x)(1+2x+5x^2+14x^3+42x^4) = O(x^5).$$

By identifying coefficients, this is equivalent to a homogeneous linear system:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 5 & 2 \\ 0 & 0 & 5 & 2 & 14 & 5 \\ 0 & 0 & 14 & 5 & 42 & 14 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \\ \gamma_1 \end{bmatrix} = 0 \iff \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 2 & 1 & 5 \\ 0 & 0 & 5 & 2 & 14 \\ 0 & 0 & 14 & 5 & 42 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \end{bmatrix} = -\gamma_1 \begin{bmatrix} 0 \\ 1 \\ 2 \\ 5 \\ 14 \end{bmatrix}.$$

By homogeneity, one can choose $\gamma_1 = 1$. Then, the violet minor shows that one can take $(\beta_0, \beta_1, \gamma_0) = (-1, 0, 0)$. The other values are $\alpha_0 = 1$, $\alpha_1 = 0$.

Thus the approximant is $(1, -1, x)$, which corresponds to $P = 1 - y + xy^2$ such that $P(x, C(x)) = 0 \bmod x^5$.

Algebraic and differential approximation = guessing

- Hermite-Padé approximants of $n = 2$ power series are related to Padé approximants, i.e. to approximation of series by rational functions
- algebraic approximants = Hermite-Padé approximants for $f_\ell = A^{\ell-1}$, where $A \in \mathbb{K}[[x]]$ seriestoalgeq, listtoalgeq
- differential approximants = Hermite-Padé approximants for $f_\ell = A^{(\ell-1)}$, where $A \in \mathbb{K}[[x]]$ seriestodiffeq, listtodiffeq

```
> listtoalgeq([1,1,2,5,14,42,132,429],y(x));
                                              2
                      [1 - y(x) + x y(x) , ogf]

> listtodiffeq([1,1,2,5,14,42,132,429],y(x));
                                     / 2        \
                     /d       \      |d         |
[{-2 y(x) + (2 - 4 x) |-- y(x)| + x |--- y(x)|, y(0) = 1, D(y)(0) = 1}, egf]
                     \dx      /      |  2       |
                                     \dx        /
```

Existence and naive computation

Theorem For any vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and for any n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, there exists a Hermite-Padé approximant of type $\mathbf{d}$ for $\mathbf{F}$.

Proof: The undetermined coefficients of $P_i = \sum_{j=0}^{d_i} p_{i,j} x^j$ satisfy a linear homogeneous system with $\sigma = \sum_i (d_i + 1) - 1$ equations and $\sigma + 1$ unknowns.

Corollary Computation in $O(\mathsf{MM}(\sigma)) = O(\sigma^\theta)$, for $2 \leq \theta \leq 3$.

▶ There are better algorithms:

- The linear system is structured (Sylvester-like / quasi-Toeplitz)
- Derksen's algorithm (Gaussian-like elimination) $O(\sigma^2)$
- Beckermann-Labahn's algorithm (DAC) $\tilde{O}(\sigma) = O(\sigma \log^2 \sigma)$

Quasi-optimal computation

Theorem [Beckermann-Labahn, 1994] One can compute a Hermite-Padé approximant of type $(d, \dots, d)$ for $\mathbf{F} = (f_1, \dots, f_n)$ in $O(\mathsf{MM}(n, d) \log(nd))$.

Ideas:

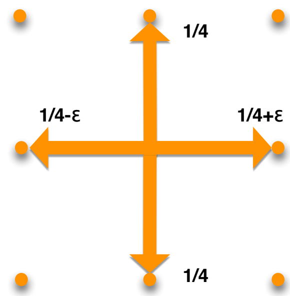
- Compute a whole matrix of approximants
- Exploit divide-and-conquer

Algorithm:

1. If $\sigma = n(d+1) - 1 \le$ threshold, call the naive algorithm
2. Else:
   (a) recursively compute $\mathbf{P}_1 \in \mathbb{K}[x]^{n \times n}$ s.t. $\mathbf{P}_1 \cdot \mathbf{F} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_1) \approx \frac{d}{2}$
   (b) compute "residue" $\mathbf{R}$ such that $\mathbf{P}_1 \cdot \mathbf{F} = x^{\sigma/2} \cdot \big(\mathbf{R} + O(x^{\sigma/2})\big)$
   (c) recursively compute $\mathbf{P}_2 \in \mathbb{K}[x]^{n \times n}$ s.t. $\mathbf{P}_2 \cdot \mathbf{R} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_2) \approx \frac{d}{2}$
   (d) return $\mathbf{P} := \mathbf{P}_2 \cdot \mathbf{P}_1$

- ▶ The precise choices of degrees is a delicate issue
- ▶ Gcd, extended gcd, Padé approximants in $O(\mathsf{M}(n) \log n)$

Example: Flea from SIAM 100-Digit Challenge




```
> proba:=proc(i,j,n,c)
option remember;
  if abs(i)+abs(j)>n then 0
  elif n=0 then 1
  else
      expand(proba(i-1,j,n-1,c)*(1/4+c)+proba(i+1,j,n-1,c)*(1/4-c)
      +proba(i,j+1,n-1,c)*1/4+proba(i,j-1,n-1,c)*1/4)
  fi
end:
> seq(proba(0,0,k,c),k=0..6);
```

$$1, 0, \frac{1}{4} - 2c^2, 0, \frac{9}{64} - \frac{9}{4}c^2 + 6c^4, 0, \frac{25}{256} - \frac{75}{32}c^2 + 15c^4 - 20c^6$$

```
> gfun:-listtodiffeq([seq(proba(0,0,2*k,c),k=0..20)],y(x));
```

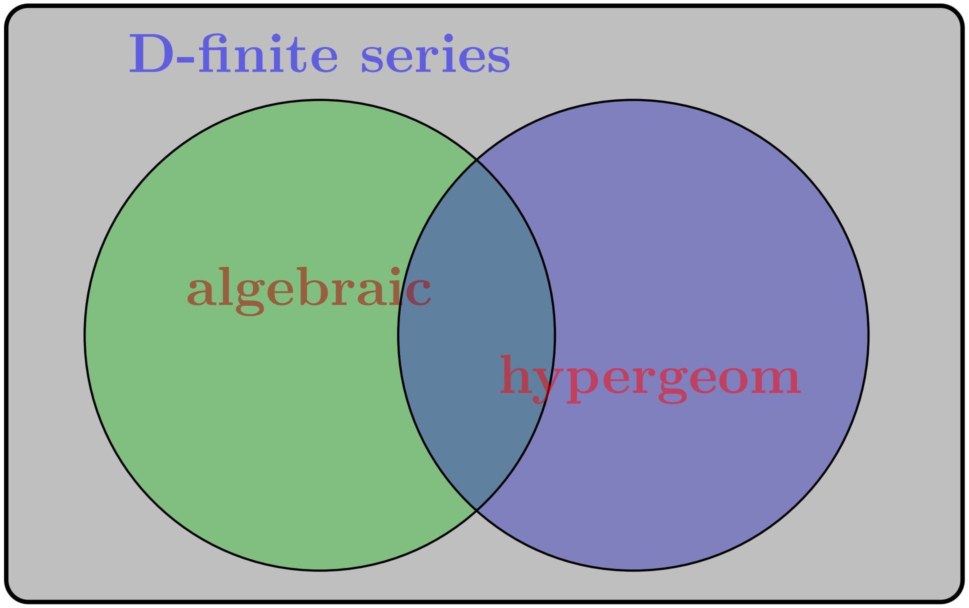
$$[\{ \left(-1+8\,c^2+48\,xc^4\right) y\left(x\right) + \left(4-8\,x+64\,xc^2+192\,x^2c^4\right) \frac{d}{dx}y\left(x\right)$$
$$+ \left(4\,x+64\,x^3c^4-4\,x^2+32\,x^2c^2\right) \frac{d^2}{dx^2}y\left(x\right),$$
$$y\left(0\right)=1, \mathrm{D}\left(y\right)\left(0\right)=1/4-2\,c^2\}, ogf]$$

Next steps: `dsolve` (+ help) and evaluation at $x = 1$.

TOOLS FOR CONJECTURES

2. p-Curvature of Differential Operators

Important classes of power series



Algebraic: $S(x) \in \mathbb{K}[[x]]$ root of a polynomial $P \in \mathbb{K}[x, y]$.

D-finite: $S(x) \in \mathbb{K}[[x]]$ satisfying a linear differential equation with polynomial (or rational function) coefficients $c_r(x)S^{(r)}(x) + \cdots + c_0(x)S(x) = 0$.

Hypergeometric: $S(x) = \sum_n s_n x^n$ such that $\frac{s_{n+1}}{s_n} \in \mathbb{K}(n)$. E.g.

$$ {}_2F_1\left(\begin{matrix} a & b \\ & c \end{matrix} \,\middle|\, x\right) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{x^n}{n!}, \quad (a)_n = a(a+1)\cdots(a+n-1). $$

Linear differential operators

Definition: If $\mathbb{K}$ is a field, $\mathbb{K}\langle x, \partial; \partial x = x\partial + 1\rangle$, or simply $\mathbb{K}(x)\langle\partial\rangle$, denotes the associative algebra of linear differential operators with coefficients in $\mathbb{K}(x)$.

$\mathbb{K}[x]\langle\partial\rangle$ is called the (rational) Weyl algebra. It is the algebraic formalization of the notion of linear differential equation with rational function coefficients:

$$a_r(x)y^{(r)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0$$

$$\Longleftrightarrow$$

$$L(y) = 0, \quad \text{where} \quad L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

The commutation rule $\partial x = x\partial + 1$ formalizes Leibniz's rule $(fg)' = f'g + fg'$.

▶ Implementation in the `DEtools` package: `diffop2de, de2diffop, mult`

```
DEtools[mult](Dx,x,[Dx,x]);
                    x Dx + 1
```

Weyl algebra is Euclidean

Theorem [Libri 1833, Brassinne 1864, Wedderburn 1932, Ore 1932]
$\mathbb{K}(x)\langle\partial\rangle$ is a non-commutative (left and right) Euclidean domain: for any $A, B \in \mathbb{K}(x)\langle\partial\rangle$, there exist unique operators $Q, R \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = QB + R, \qquad \text{and} \quad \deg_\partial(R) < \deg_\partial(B).$$

This is called the Euclidean right division of A by B.

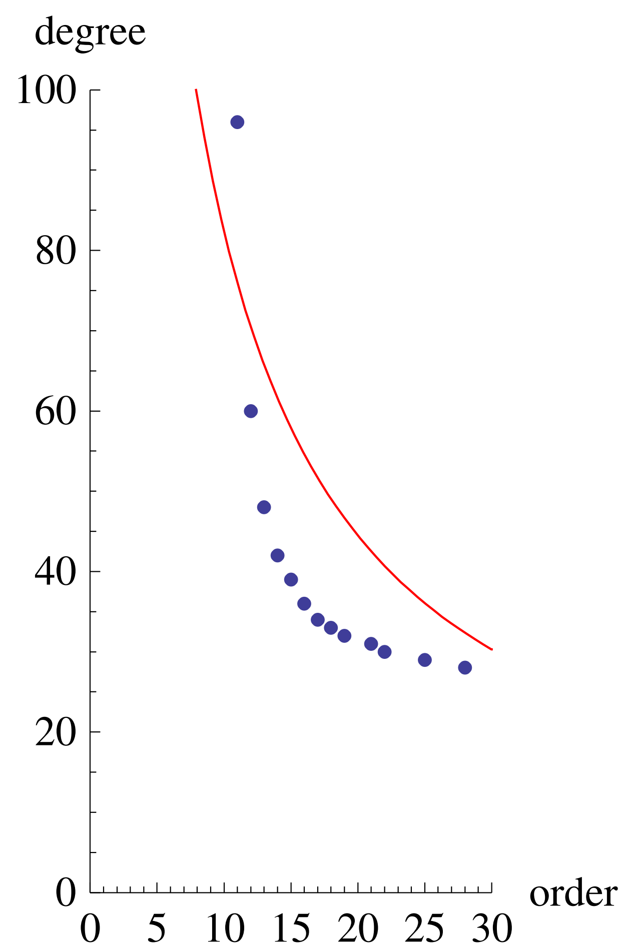
Moreover, any $A, B \in \mathbb{K}(x)\langle\partial\rangle$ admit a greatest common right divisor (GCRD) and a least common left multiple (LCLM). They can be computed by a non-commutative version of the extended Euclidean algorithm.

▶ `rightdivision, GCRD, LCLM` from the `DEtools` package

```
> rightdivision(Dx^10,Dx^2-x,[Dx,x])[2];
                              3                  2    5
                        (20 x  + 80) Dx + 100 x  + x
```

proves that $\mathrm{Ai}^{(10)}(x) = (20x^3 + 80)\mathrm{Ai}'(x) + (100x^2 + x^5)\mathrm{Ai}(x)$

Application to differential guessing



1000 terms of a series are enough to guess candidate differential equations below the red curve. GCRD of candidates could jump above the red curve.

The Grothendieck–Katz p-curvatures conjecture

Q: when does a differential equation possess a basis of algebraic solutions?

E.g. for the Gauss hypergeometric equation $x(1-x)\partial^2 + (\gamma - (\alpha+\beta+1)x)\partial - \alpha\beta x$, Schwarz's list (1873) classifies algebraic ${}_2F_1$'s in terms of α, β, γ

Conjecture [Grothendieck, 1960's, unpublished; Katz, 1972]
Let $A \in \mathbb{Q}(x)^{n\times n}$. The system (S) : $y' = Ay$ has a full set of algebraic solutions if and only if, for almost all prime numbers p, the system (S$_p$) defined by reduction of (S) modulo p has a full set of algebraic solutions over $\mathbb{F}_p(x)$.

Definition: The p-curvature of (S) is the matrix A_p, where

$$A_0 = I_n, \quad \text{and} \quad A_{\ell+1} = A_\ell' + A_\ell A \quad \text{for} \quad \ell \geq 0.$$

Theorem [Cartier, 1957]
The sufficient condition of the G.-K. Conjecture is equivalent to $A_p = 0 \bmod p$.

- For each p, this can be checked algorithmically.

Grothendieck's conjecture

Q: when does a differential equation possess a basis of algebraic solutions?

For a scalar differential equation, the G.-K. Conjecture can be reformulated:

Grothendieck's Conjecture: Suppose $L \in \mathbb{K}(x)\langle\partial\rangle$ is irreducible. The equation (E) : $L(y) = 0$ has a basis of algebraic solutions if and only if, for almost all prime numbers p, the operator L right-divides ∂^p modulo p.

- For each p, this can be checked algorithmically.

- Conjecture is proved for Picard-Fuchs equations [Katz 1972] (in particular, for diagonals [Christol 1984]), for ${}_nF_{n-1}$ equations [Beukers & Heckman 1989].

Grothendieck's conjecture for combinatorics

Suppose that we have guessed a linear differential equation $L(f) = 0$ (by differential Hermite-Padé approximation) for some power series $f \in \mathbb{Q}[[x]]$, and that we want to recognize whether f is algebraic or not.

Recipe 1: try algebraic guessing.

Recipe 2: For several primes p, compute p-curvatures mod p, and check whether they are zero; equivalently, test if $\partial^p \bmod L = 0 \pmod{p}$.

► For many power series coming from counting problems (diagonals, constant terms, integrals of algebraic functions, ...) Grothendieck's conjecture is true.

Grothendieck's conjecture at work

Chebychev in his work on the distribution of primes numbers used the following fact

$$u_n := \frac{(30n)!n!}{(15n)!(10n)!(6n)!} \in \mathbb{Z}, \qquad n = 0, 1, 2, \ldots$$

This is not immediately obvious (for example, this ratio of factorials is not a product of multinomial coefficients) but it is not hard to prove. The only proof I know proceeds by checking that the valuations $v_p(u_n)$ are non-negative for every prime p; an interpretation of u_n as counting natural objects or being dimensions of natural vector spaces is far from clear.

As it turns out, the generating function

$$u := \sum_{\nu \geq 1} u_n \lambda^n$$

is algebraic over $\mathbb{Q}(\lambda)$; i.e. there is a polynomial $F \in \mathbb{Z}[x, y]$ such that

$$F(\lambda, u(\lambda)) = 0.$$

However, we are not likely to see this polynomial explicitly any time soon as its degree is $483,840$ (!)

(excerpt from Rodriguez-Villegas's "Integral ratios of factorials")

- Algebraicity of u can be however guessed using any prior knowledge, by computing p-curvatures of the (minimal) order-8 operator L s.t. $L(u) = 0$
- For $p < 300$, they are all zero, except when $p \in \{11, 13, 17, 19, 23\}$

G-series and global nilpotence

Definition: A power series $\sum_{n\geq 0} \frac{a_n}{b_n} x^n$ in $\mathbb{Q}[[x]]$ is called a G-series if it is (a) D-finite; (b) analytic at $x = 0$; (c) $\exists\, C > 0$, $\operatorname{lcm}(b_0, \ldots, b_n) \leq C^n$.

Basic examples: (1) algebraic functions [Eisenstein 1852]

(2) $-\log(1 - x) = \sum_{n\geq 1} x^n/n$ ([Chebyshev 1852] $\operatorname{lcm}(1, 2, \ldots, n) \leq 4^n$)

(3) ${}_2F_1\left(\begin{matrix}\alpha \;\; \beta \\ \gamma\end{matrix} \,\middle|\, x\right)$, $\alpha, \beta, \gamma \in \mathbb{Q}$

(4) OGF of any P-recursive, integer-valued, exponentially bounded, sequence

Theorem [Chudnovsky 1985] The minimal-order linear differential operator annihilating a G-series is globally nilpotent: for almost all prime numbers p, it right-divides $\partial^{p\mu}$ modulo p, for some $\mu \leq \deg_\partial L$.
(this condition is equivalent to the nilpotence mod p of the p-curvature matrix)

Examples: algebraic resolvents; Gauss's $x(1 - x)\partial^2 + (\gamma - (\alpha + \beta + 1)x)\partial - \alpha\beta x$.

Global nilpotence for combinatorics

Suppose we have guessed (by differential approximation) a linear differential equation $L(f) = 0$ for a power series $f \in \mathbb{Q}[[x]]$ which is a G-series (typically, the OGF of a P-recursive, integer-valued, exponentially bounded, sequence).

A way to empirically certify that L is very plausible:

Recipe: compute p-curvatures mod p, and check whether they are nilpotent; equivalently, test if $\partial^{pr} \bmod L = 0 \pmod p$, where $r = \deg_\partial L$

Example:

```
> L:=x^2*(64*x^4+40*x^3-30*x^2-5*x+1)*Dx^3+
      x*(576*x^4+200*x^3-252*x^2-33*x+5)*Dx^2+
       4*(1+288*x^4+22*x^3-117*x^2-12*x)*Dx+384*x^3-12-144*x-72*x^2:
> p:=7; for j to 3 do N:=rightdivision(Dx^(3*p),L,[Dx,x])[2] mod p;
        p:=nextprime(p); print(p, N); od:

                                  11, 0
                                  13, 0
                                  17, 0
```

Overview

Today

1. Introduction
2. High Precision Approximations
   – Fast multiplication, binary splitting, Newton iteration
3. Tools for Conjectures
   – Hermite-Padé approximants, p-curvature

Tomorrow morning

4. Tools for Proofs
   – Symbolic method, resultants, D-finiteness, creative telescoping

Tomorrow night

– Exercises with Maple